Inserta el logotipo de tu institución

Taller Federación de Identidades

Módulo I

Fernando Aranda – CUDI, A.C.

Juan Gabriel Cruz Pérez - UCOL

Puerto Vallarta, Jalisco, del 29 de mayo al 02 de junio

CUDI – FENIX - FONCICYT

- La investigación realizada por CUDI y que lleva a estos resultados ha recibido financiamiento de FONCICYT, bajo el Acuerdo 4/II/2014 con el que se autorizó la asignación de recursos para apoyar la Segunda Convocatoria para el registro de pre-propuestas CONACYT Horizon2020 y mediante acuerdo número 15/IVE/2015, del Comité Técnico y de Administración del "FONCICYT", autorizando la canalización de recursos a favor de CUDI para el desarrollo del proyecto denominado "Middleware for Collaborative Applications and Global VIrtual Communities". A su vez se fundamenta en los resultados obtenidos del financiamiento otorgado por el Séptimo Programa Marco (FP7 2007-2013) de la Comunidad Europea, bajo el Acuerdo de Subvención No. 238875 (GÉANT).

FENIX

- **FE**deración **N**acional de **I**dentidades Me**X**icana (**FENIX**) http://www.fénix.org.mx
- **FENIX** es una Iniciativa de CUDI para crear una Federación de Identidades en México
- El proyecto inició en 2014 con **FIDMEX**
- El objetivo principal de **FENIX** es sumar a todas las universidades e instituciones de investigación mexicanas a la Federación
- Para la construcción de la federación se utilizaron soluciones de software y estándares ya disponibles y adoptados por otras federaciones

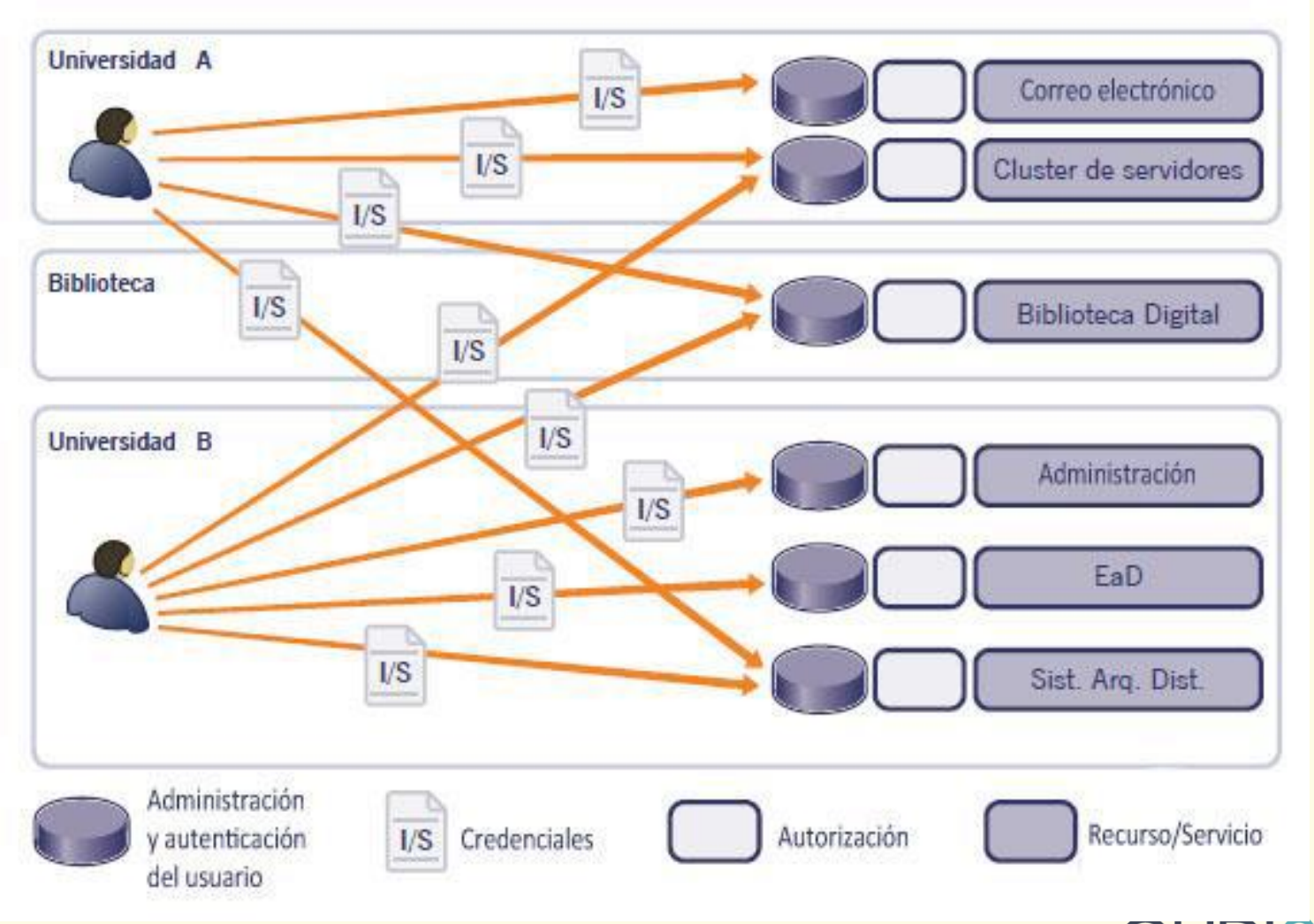
Hoja de Ruta

- **Módulo I**: Introducción a los entornos federado de los ambientes educativos, que son, beneficios y ejemplos.
- **Módulo II**: Como instalar y desplegar un Proveedor de Identidad (IdP), un Proveedor de Servicio (SP) y federar un servicio de prueba, utilizando el protocola SAML 2.
- **El Módulo III**: Como utilizar diferentes fuentes de datos, aplicar filtros, manejar el consentimiento de los usuarios, metarefresh

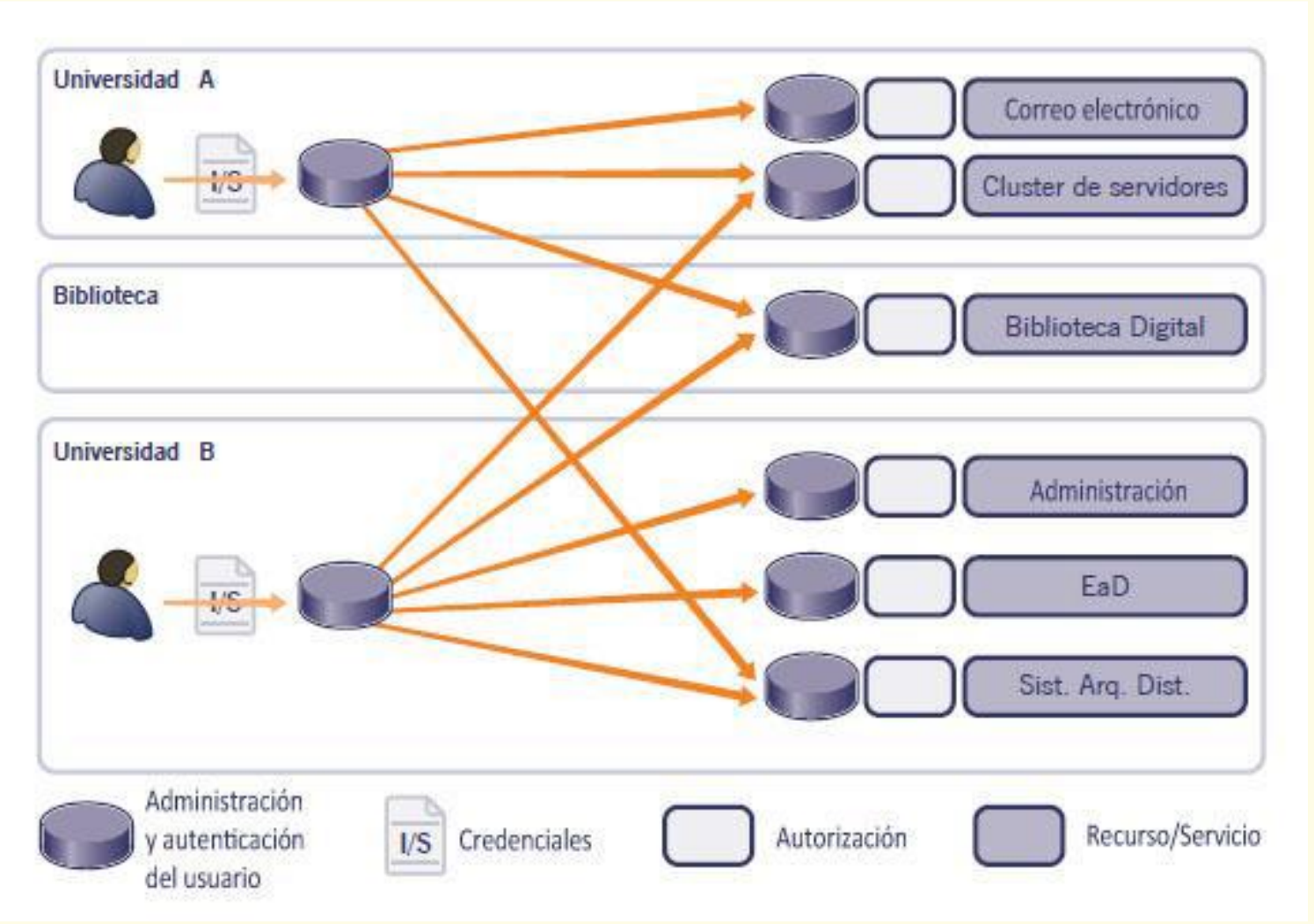
Módulo I - Fundamentos

- ¿Qué es una federación?
- Una federación es una red de confianza
- Una federación ofrece a las instituciones la infraestructura de **autenticación** y **autorización**
- Utiliza el principio de identidad federada, donde las instituciones implementan diferentes métodos de autenticación, manteniendo la interoperabilidad
- La **autenticación** es el proceso de verificar la identidad de una persona
- La **autorización** es el proceso de verificación de que una persona ya identificada tenga la autoridad para realizar una cierta operación o para acceder a un cierto servicio o recurso

Sistema Tradicional



Sistema Federado



Beneficios

- Menor costo de mantenimiento del servicio y de las cuentas de usuario
- Utiliza el sistema de autenticación que tiene su Institución
- Acceso a servicios externos
- Se cierra sesión una sola vez

FENIX

CUDI 2017
PUERTO VALLARTA

Elementos de una Federación

- Proveedor de Identidad (IdP)
- Proveedor de Servicio (SP)
- Servicio de Descubrimiento (DS / WAYF)

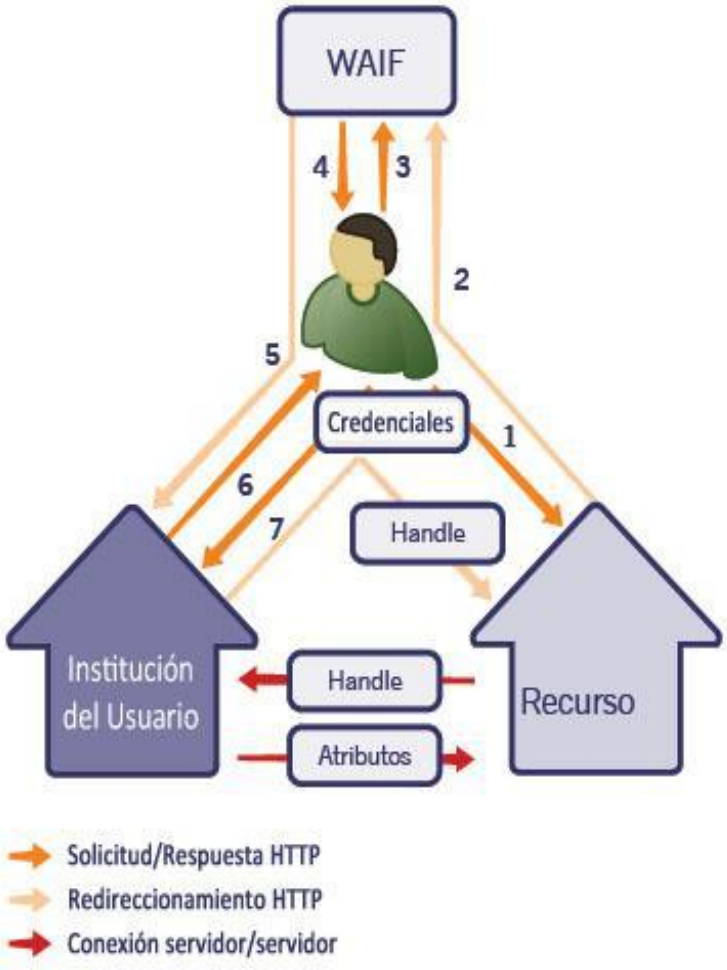
Proveedor de Identidad (IdP)

- Implementa una política interna de gestión de identidad
  - Atributos de los usuarios: Nombre, fecha nacimiento, cargo, ID.
- Método de autenticación.
  - Login / contraseña, certificados digitales, etc.
- Otorga un identificador único para cada usuario de la institución

Proveedor de Servicio (SP)

- Implementa los servicios que deben estar disponibles para los usuarios de las instituciones y requieren:
  - Autenticación, identificación de los usuarios
  - Autorización, atributos adicionales que garantizan ciertos privilegios de acceso.
- Su enfoque está en la implementación del servicio y no en el mantenimiento de los registros de los usuarios

Interacción entre los elementos de la FI



- **1:** El usuario accede al proveedor de servicio **(SP)**.
- **2:** El servicio presenta opciones del **DS/WAYF** centralizado.
- **3:** El usuario selecciona su institución de origen.
- **4:** El usuario es redirigido hacia su (IdP).
- **5:** El **IdP** autentica al usuario con el método elegido por la institución.
- **6:** El **SP** recibe la garantía de autenticación del usuario de parte del **IdP**.
- **7:** El **SP** pide atributos adicionales de ese usuario al **IdP**; para garantizar la privacidad del usuario, sólo se entregan atributos previamente acordados entre el **IdP** y el **SP**.
- **8:** El proveedor de servicio decide sobre las autorizaciones y proporciona el servicio al usuario.

Ejemplos de Federaciones

- http://www.rediris.es/sir/
- https://www.rnp.br/servicos/servicos-avancados/cafe
- http://cofre.reuna.cl/index.php/es/
- http://www.incommon.org/federation/
- http://services.geant.net/edugain/Pages/Home.aspx